Preparing to Face Today’s Risks & Hazards: Is Your Organization Ready?

Knowing What to Do Before, During and After a Disaster is the Key to Continuity of Operations

By Bob Mellinger

Organizations today need a comprehensive, integrated plan in place to protect people, property, technology, and, to the greatest degree possible, their reputation and financial viability in the face of a myriad of risks. Your disaster response and business continuity plans should cover as much as feasible and make business recovery possible. Overriding all, however, is personal safety and the need to preserve life. These are always the top priorities.

It’s not just terrorism, natural and man-made disasters, legal liability (injury, violence, etc.), and government regulations that threaten your operations. Consider these actual events and their potential impacts:

- Your web server is the target of a distributed denial-of-service (DDoS) attack
- 150 protestors block the entrance to the hotel site on the opening day of your national conference; a large number of them stage a sit-down protest in the main lobby/registration area.
- A newly fired employee returns to the workplace with a gun and starts shooting. Do you have a plan to deal with an active shooter on the premises?
- It’s Friday afternoon and you get a call from your primary cloud provider to inform you that they are shutting down operations immediately. What now? Do you have a Plan B?

Reputation damage, litigation, and other factors increase the odds against business survival; there is significant potential for loss of income if you are not prepared. It’s entirely possible that one ruined or badly-handled incident might result in extensive revenue losses and require years of rebuilding reputation.

The First Step

Before anything happens, the most critical activity you undertake is planning. Knowing what to plan for is the first challenge. How do you plan for and survive disruptions you can only imagine? It’s not possible to be prepared for every possible situation; you have to concentrate on those that are most likely to occur. It’s vital to determine the risk of each potential disruption and to decide on which to concentrate your resources.

Most important is to keep things in perspective. Any consequence that involves potential critical injury or loss of life must take precedence over less critical outcomes. It’s necessary, therefore, to prioritize the risks as well as to identify the ones on which to focus. You can do that by using a “what-if” approach.

Ask yourself, “What if...?” What if a part of the roof collapsed? What if the keynote speaker died in mid-sentence? What if the chairman of the board was taken hostage? Develop a comprehensive list of such threats that you can then use to go through the planning process. This is the age-old problem/solution approach to planning and is a good way to start. Does your organization have unique threat potential due to its location or climate? Are there groups that take issue with your practices or beliefs, or those of your clients? Also, what is a threat this month may not be a threat next month, so you have to continually review the current situation.

Mitigation: Isn’t it better if the disruption never occurs?

Mitigation is everything you do to prevent a disruption from occurring or to minimize its impact. It’s planning early and carefully for security if you are hosting a high-visibility individual. It’s having a tested backup and recovery facility for your critical operations in case a broken gas line shuts down your building. It’s having at least one plain old telephone that gets its power from the Telco line versus an electrical outlet.

Mitigation activities can be identified by reviewing your vulnerabilities and/or plans to determine what can be done NOW as opposed to waiting for a disruption. This kind of planning is one of the best ways to help ensure that your operations can continue without significant disruption.

Response

The response period begins at the start of the disrupting event and continues until the situation has been stabilized. You need to build response capability into your plans in order to minimize the immediate impact of any disruption. If you have a meeting scheduled at a local hotel (where your attendees and staff are also staying), and the hotel burns down while they’re at a luncheon several blocks away, what are you going to do? The hotel ultimately is responsible, but you can’t tell your attendees it’s not your problem. At the very least, you need to provide assistance in dealng with the hotel and their contingency plans. In addition, you may need to get on the phone and assist the members in finding other accommodations and helping them figure out how to replace personal belongings and lost medications.

You can best handle the response to any disruption if, in your planning, you created a crisis response team that you can call into play. Just as you can’t possibly plan for every vulnerability, you can’t possibly pre-empt responses when unexpected disruption occurs. But you can transform other plans to help you deal with this, and you can hold drills to practice working under pressure and as a team. You also need a designated spokesperson—someone who will deal with the media (when necessary) and other groups confidently and forthrightly.

One thing to remember about responding to threats and hazards is that, despite different causes, the general flow of activities is similar. There is an “all hazards approach”: try to save people, secure the situation, get everything under control.

How soon can we operate again?

After any disruption, all we want is for things “to get back to normal,” but this seldom happens. There is usually a “new” normal after a disruption. Things have changed. Some classic examples of this are the impacts of Hurricanes Harvey, Irma and Maria and the Las Vegas shooting. Businesses and homes damaged by the hurricanes may take months or years to be repaired, and many businesses may never reopen. There’s no real estimate of when power will be restored in Puerto Rico and the US Virgin Island. The shooting in Las Vegas will create a new normal for many concerts in terms of where they are located and the security required.

We want actions in the recovery stage to enable us to minimize the long-term impact of the disruption on the organization. In the case of a food poisoning incident, for example, recovery might mean immediately inviting health officials to investigate, getting in a new vendor for any remaining meals and publicizing this to your members personally and via the media. The food poisoning wasn’t your fault, but your reputation is at risk regardless.

While each situation has its unique risks, your overall plan does not have to be reinvented for each situation. You can easily customize your planning to incorporate the mitigation and response required for varying situations. Just remember that, in each instance, you need specifically to consider any risks that could significantly impact you or your members’ safety and reputation.
"Before anything happens, the most critical activity you undertake is planning. Knowing what to plan for is the first challenge. How do you plan for and survive disruptions you can only imagine? It’s not possible to be prepared for every possible situation; you have to concentrate on those that are most likely to occur. It’s vital to determine the risk of each potential disruption and to decide on which to concentrate your resources."

**Awareness and Training**

The important final step in this planning process is ensuring that everyone is aware of the plan and can follow it. You must test the plan regularly to keep it current and ensure its viability. What happens, for example, when a disruption occurs and all of a sudden you discover that the person in charge of a critical piece left the company six months ago? Finally, the plan has to be easy to use. Don’t make it easier for people to run for the door than to locate the correct procedure in the plan (of course, if the plan is tested and people are trained, this shouldn’t be an issue).

**Summary**

The job of business continuity is an overwhelming one, particularly when viewed from the perspective of planning to survive the threats and hazards that can impact organizations today. Planning is the key to making it through. The risk assessment process can help you identify and prepare for the myriad of disruptions you might face. Mitigation activities actually can reduce certain threats. Response plans that are communicated effectively mean that everyone knows their role in the event of any disruption. Recovery plans help reduce the amount of downtime to the facility. And training, testing and evaluation are critical to keeping plans accessible, current, and effective.

Bob Mellinger is the President of Attainium Corp. He can be reached at bmellinger@attainium.net. Bob presented the course, The Disaster Experience – Before, During and After at Association Forum on January 25, 2018.